ATTACHMENT 2

Model Security Plan for Prohibited Technologies

Date: Jan 26, 2023

Version: 1.0

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND:

On December 7, 2022, Governor Greg Abbott required (https://gov.texas.gov/uploads/files/press/State_Agencies_Letter_1.pdf) all state agencies to ban the video-sharing application TikTok from all state-owned and state-issued devices and networks over the Chinese Communist Party's ability to use the application for surveilling Texans. Governor Abbott also directed the Texas Department of Public Safety (DPS) and the Texas Department of Information Resources (DIR) to develop a plan providing state agencies guidance on managing personal devices they use to conduct state business.

SCOPE:

This plan applies to all state agencies and institutions of higher education (IHEs), including their employees, contractors, interns, or any users of state-owned networks. Each agency is responsible for the implementation of the plan as outlined in this document, including any changes to meet specific agency needs.

OBJECTIVES

To protect the State's sensitive information and critical infrastructure from technology that poses a threat to the State of Texas, this plan outlines the following objectives for each agency:

1. Ban and prevent the download or use of prohibited technologies on any state-issued device. This includes all state-issued cell phones, laptops, tablets, desktop computers, and other devices of capable of internet connectivity. Each agency's IT department must strictly enforce this ban.
2. Prohibit employees or contractors from conducting state business on prohibited technology-enabled personal devices.
3. Identify sensitive locations, meetings, or personnel within an agency that could be exposed to prohibited technology-enabled personal devices. Prohibited technology-enabled personal devices must be prohibited from entering or being used in these sensitive areas.

4. Implement network-based restrictions to prevent the use of prohibited technologies on agency networks by any device.
5. Coordinate the incorporation of other technology providers as necessary, including any apps, services, hardware, or software that pose a threat to the State's sensitive information and critical infrastructure into this plan.

STATE AGENCY SECURITY PLAN

OBJECTIVE 1: PROHIBIT THE DOWNLOAD AND USE OF PROHIBITED TECHNOLOGIES ON ANY STATE-ISSUED DEVICE.

Prohibited technologies shall not be downloaded or used on any state-issued device. This includes all state-issued cell phones, laptops, tablets, desktop computers, or any other devices of capable of internet connectivity. Each agency must strictly enforce this objective.

To achieve this security plan objective, agencies must implement the following:

1. Agencies must identify, track, and control state-owned devices to prohibit the installation of or access to all prohibited technologies. This includes the various applications for mobile, desktop, or other internet capable devices.
2. Determine if prohibited technologies have been downloaded on state-issued devices. If so, the agency must remove the application from those devices immediately unless an exception has been granted in writing by the agency head and reported to DIR.
3. Configure agency network firewall(s) to block prohibited domains on both the local network and virtual private network (VPN).
4. Manage all state-issued mobile devices by implementing the security controls listed below:
    a. Restrict access to "app stores" or non-authorized software repositories to prevent the installation of unauthorized applications.
    b. Maintain the ability to remotely wipe non-compliant or compromised mobile devices.
    c. Maintain the ability to remotely uninstall un-authorized software from mobile devices.

d. Deploy secure baseline configurations, for mobile devices, as determined by the agency.

OBJECTIVE 2: PROHIBIT EMPLOYEES AND CONTRACTORS FROM CONDUCTING STATE BUSINESS ON PROHIBITED TECHNOLOGY-ENABLED PERSONAL DEVICES.

In addition to preventing the use of prohibited technologies on state-issued devices, agencies must prohibit employees and contractors from using prohibited technology-enabled personal devices to conduct state business. State business includes accessing any state-owned data, applications, email accounts, or non-public facing communications. Examples of state network resources include state email, VoIP, SMS, video conferencing, CAPPS, Texas.gov, and any other state databases or applications.

If an agency has a justifiable need to allow the use of personal devices to conduct state business, the agency may establish a "Bring Your Own Device" (BYOD) program with the following considerations:

a. Ability to manage lost, stolen, or unauthorized devices;
b. Prevent the installation of banned or unauthorized software;
c. Prevent the use of unsecure public networks;
d. Manage open records, confidentiality, and privacy-related issues;
e. Ability to create a guest security profile that prevents prohibited technologies from communicating or being downloaded while that security profile is in use; and
f. Ability to remove all state-related business and applications from the personal device before removing the security profile or un-enrolling the device from the BYOD program.

OBJECTIVE 3: IDENTIFY SENSITIVE LOCATIONS, MEETINGS, AND PERSONNEL WITHIN AN AGENCY THAT COULD BE EXPOSED TO PROHIBITED TECHNOLOGY-ENABLED PERSONAL DEVICES.

1. Agencies must identify, catalog, and label sensitive locations within the agency. A sensitive location is any location, physical, or logical (such as video conferencing, or electronic meeting rooms) that is used to discuss confidential or sensitive information, including information technology configurations, criminal justice

information, financial data, personally identifiable data, sensitive personal information, or any data protected by federal or state law.

2. Agencies must indicate when someone is entering a sensitive location. Physical locations should have exterior signage, and electronic meetings should be labeled.
3. Unauthorized devices, such as personal cell phones, tablets, or laptops, may not enter sensitive locations. This includes any electronic meeting labeled as a sensitive location. Locked storage areas that prevent external communications with the devices stored within may be placed outside of sensitive locations to temporarily hold unauthorized devices when entering a sensitive location.
4. Visitors granted access to secure locations are subject to the same limitations as contractors and employees on unauthorized personal devices when entering secure locations. Agencies are responsible for securing sensitive areas.

OBJECTIVE 4: IMPLEMENT NETWORK-BASED RESTRICTIONS TO PREVENT THE USE OF PROHIBITED TECHNOLOGIES ON AGENCY NETWORKS BY ANY PROHIBITED TECHNOLOGY-ENABLED PERSONAL DEVICE.

DIR Cyber Operations has blocked access to prohibited technologies on the state network. To ensure multiple layers of protection, agencies must also implement additional network-based restrictions to prevent communication with prohibited internet services:

1. Agencies must configure firewalls to block access to statewide prohibited services on all agency technology infrastructures, including local networks, WAN, and VPN connections.
2. Agencies must prohibit personal devices with prohibited technologies installed from connecting or attempting to connect to agency or state technology infrastructure or state data.
3. Agencies may provide access to prohibited technologies through a separate network, with the approval of the agency head.

OBJECTIVE 5: COORDINATE THE INCORPORATION OF ANY ADDITIONAL TECHNOLOGY THAT POSES A THREAT TO THE STATE'S SENSITIVE INFORMATION AND CRITICAL INFRASTRUCTURE INTO THIS PLAN.

To provide protection against ongoing and emerging technology threats to the state's sensitive information and critical infrastructure, technologies will be regularly monitored and evaluated for inclusion into this plan.

1. DPS and DIR will evaluate and monitor technologies that pose a threat to state sensitive information and critical infrastructure. They will provide recommendations to state leaders on technologies that should be blocked or prohibited statewide.
2. DIR will host a site (https://dir.texas.gov/information-security/prohibited-technologies) that lists all technologies including apps, software, hardware, or technology providers that are prohibited. New technologies will be added to the list after consultation between DIR and DPS.
3. DIR will notify agencies in the event the list is amended.
4. It is the responsibility of each agency to implement the removal and prohibition of any offending technology.
5. The prohibited technologies list current as of January 23, 2023, can be found in Addendum A.

EXCEPTIONS

Exceptions may only be approved by the head of the agency to enable law-enforcement investigations or other legitimate business uses. This authority may not be delegated. All approved exceptions to allow the use of a prohibited technology must be reported to DIR.

Devices granted an exception should only be used for the specific use case in which the exception was granted and only used on non-state or specifically designated separate networks. If possible, cameras and microphones should be disabled on those devices when not in active use for their intended purpose.

For personal devices used for state business, exceptions should be limited to extenuating circumstances and only granted for a pre-defined period of time.

IHEs may include an exception to accommodate student use of a state email address provided by the university in the policy submitted to DPS. Any such exception shall be restricted to student's use of a personal device that is privately owned or leased by the student or a member of the student's immediate family, and shall include network security considerations to protect the IHE network and data from traffic related to prohibited technologies.

PLAN COMPLIANCE

Each agency is required to develop its own security policy to support the implementation of this plan. This policy must be submitted by February 15, 2023 to the Department of Public Safety by uploading the document to the SPECTRIM portal. The SPECTRIM portal will be configured to receive these policies by February 1, 2023.

ADDENDUM A

The up-to-date list of prohibited technologies is published at https://dir.texas.gov/information-security/prohibited-technologies. The following list is current as of January 23, 2023.

Prohibited Software/Applications/Developers

- TikTok
- Kaspersky
- ByteDance Ltd.
- Tencent Holdings Ltd.
- Alipay
- CamScanner
- QQ Wallet
- SHAREit
- VMate
- WeChat
- WeChat Pay
- WPS Office
- Any subsidiary or affiliate of an entity listed above.

Prohibited Hardware/Equipment/Manufacturers

- Huawei Technologies Company
- ZTE Corporation
- Hangzhou Hikvision Digital Technology Company
- Dahua Technology Company
- SZ DJI Technology Company
- Hytera Communications Corporation
- Any subsidiary or affiliate of an entity listed above.